UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/576,516	05/23/2000	Xin Qiu	18926-002110US	4301

20350 7590 12/22/2003

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/22/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/576,516	QIU ET AL.	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-32 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-32 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-32 rejected under 35 U.S.C. 102(b) as being anticipated by Grube et al.

3. As per claim 1, Grube et al. discloses a method of providing varying levels of security in a data processing system(405)(see fig. 4, sheet 3, col. 2, lines 39-57), receiving information from an outside source(see col. 2, lines 58-67, col. 3, lines 1-20); retrieving an indicator from the received information that instructs the system to operate at a higher level of security(see col. 3, lines 39-62, col. 5, lines 25-38). Grube et al. discloses to prevent operation at a lower level of security until information is received by the system to authorize a decrease in security levels, because if the acknowledgement is not received, or if the acknowledgement was not constructed with the proper transmission security level parameters, then the process ends(see col. 7, lines 53-65).

4. As per claim 2, the same motivation applies above, also, Grube et al. discloses receiving an encrypted message(see col. 4, lines 7-20).

5. As per claim 3, Grube et al. discloses wherein said Decreased-Security Authorization-Code authorizes a decrease in encryption/decryption levels(see col. 3, lines 45-65).

6. As per claim 4, Grube et al. discloses wherein said Decreased-Security Authorization-Code authorizes a decrease in authentication level(see col. 3, lines 45-65).

7. As per claim 5, Grube et al. discloses wherein said Decreased-Security Authorization-Code authorizes a decrease in authentication level and a decrease in encryption/decryption levels(see col. 3, lines 45-65).

8. As per claim 6, Grube et al. discloses wherein said encrypted message further comprises a key for use in a decryption algorithm(see col. 4, lines 7-45).

9. As per claim 7, stores a master key(i.e. unique user key) to decrypt messages includes new decryption key values and using said master key stored at said system to decrypt said encrypted message(see col. 3, lines 59-67, col. 4, lines 1-45).

10. As per claim 8, Grube et al. discloses establishing a Security-Level-Status-Indicator at said system to indicate a level of security that is being implemented(see fig. 3, sheet 2).

11. As per claim 9, Grube et al. discloses said Security-Level-Status Indicator indicates a level of encryption/decryption that is being implemented by the system(see fig. 3, sheet 2, col. 3, lines 59-65, col. 5, lines 26-44).

12. As per claim 10, Grube et al. discloses said Security-Level-Status Indicator indicates a level of authentication that is being implemented by the system(see col. 3, lines 59-67).

13. As per claim 11, said Security-Level-Status Indicator indicates a level of authentication and a level of encryption/decryption that is being implemented by the system(see col. 3, lines 45-65).

14. As per claim 12, Grube et al. does not disclose configuring said Security Level Status Indicator to indicate more than two security levels so as to allow said system to utilize more than two security levels; however, the Examiner asserts that it would have been obvious to include

Grube et al. to have more than two security levels, the motivation is that it increases security of the communication unit of Grube.

15. As per claim 13, Grube et al. does not disclose utilizing a cable head-end as said outside source; however, the Examiner asserts that it would have been obvious to utilize a cable head-end as an outside source, the motivation is that a cable head-end provides faster transmission.

16. As per claim 14, Grube et al. discloses using a Key Management Message to convey said Decreased Security Authorization Code(see col. 3, lines 45-65).

17. As per claim 15, Grube et al. discloses wherein delivery of said Key Management Message is authenticated(see col. 36-47).

18. As per claim 16, Grube et al. discloses wherein delivery of said Key Management Message is protected against a replay attack(see col. 7, lines 35-65).

19. As per claim 17, Grube et al. discloses wherein delivery of said Key Management Message is authenticated and protected against a replay attack(see col. 8, lines 1-30).

20. As per claim 18, Grube et al. discloses wherein a lower level of security is nonpublic Key mode, wherein a higher level of security is a public Key mode, continuing operation of the system in the public Key mode until an encrypted predefined message is received by the system from the outside source(see col. 3, lines 53-65).

21. As per claim 19, rejected under the same basis as claim 7.

22. As per claim 20, recites limitations already rejected(see claims 1 and 12).

23. As per claim 21, Grube et al. discloses a cryptographic device an input to receive a datastream; a Security -Level-Status-Indicator; and code means for executing a cryptographic

algorithm wherein said cryptographic algorithm is indicated by said Security-Level-Status-Indicator(see col. 3, lines 59-67, col. 5, lines 26-44, fig. 3, sheet 2).

24. As per claim 22, Grube et al. discloses wherein said code means for executing a cryptographic algorithm comprises code means for executing a high level cryptographic algorithm and code means for executing a low level cryptographic algorithm relative to said high level cryptographic algorithm(see fig. 3, lines 59-67).

25. As per claim 23, Grube et al. discloses wherein said high level cryptographic algorithm comprises a high level decryption algorithm and wherein said low level cryptographic algorithm comprises a low level decryption algorithm(see col. 3, lines 53-65).

26. As per claim 24, Grube et al. discloses wherein said high level cryptographic algorithm comprises a high level authentication algorithm and wherein said low level cryptographic algorithm comprises a low level authentication algorithm(see col. 7, lines 24-35).

27. As per claim 25, Grube et al. discloses wherein said high level cryptographic algorithm comprises a high level decryption algorithm and a high level authentication algorithm and wherein said low level cryptographic; algorithm comprises a low level decryption algorithm and a low level authentication algorithm(see col. 3, lines 59-67, col. 7, lines 24-35) .

28. As per claim 26, Grube et al. discloses wherein said high level cryptographic algorithm is a public Key encryption algorithm and wherein said low level cryptographic algorithm is a non-public Key encryption algorithm(see col. 3, lines 53-65).

29. As per claim 27, Grube et al. discloses means for decrypting a decreased security Authorization Code(see col.7, lines 24-35).

30. As per claim 28, Grube et al. discloses and means for preventing a replay attack in delivery of said Decreased-Security Authorization-Code(see col. 8, lines 1-30).

31. As per claim 29, Grube et al. discloses a master key to use in decrypting said Decreased Security Authorization Code(see col. 3, lines 59-67, col. 4, lines 1-45).

32. As per claim 30, Grube et al. discloses wherein said Security Level Status Indicator is encrypted(see col.7, lines 36-50).

33. As per claim 31, Grube et al. discloses providing a receiver to receive a transmission(see col. 2, lines 58-67, col. 3, lines 1-20); establishing a Security-Level-Status-Indicator at said receiver(see col. 3, lines 59-67); establishing a first level of decryption at said receiver(see col. 3, lines 59-67, col. 4, lines 1-20); encrypting a first message at a first level of encryption(see col. 3, lines 59-67, col. 4, lines 1-20); transmitting said first message to said receiver at said first level of encryption(see col. 2, lines 58-67, col. 3, lines 1-20); receiving said first message at said receiver(see col. 7, lines 36-65); decrypting said first message encrypted at said first level of encryption(see col. 7, lines 36-65); transmitting a Decreased-Security-Authorization Code to change from said first level of decryption to a second level of decryption(see col. 3, lines 12-58); receiving said Decreased-Security-Authorization-Code; determining a change in encryption level from said first level of encryption to said second level of encryption(see fig. 3, lines 59-67, col. 4, lines 1-20); adjusting said Security-Level-Status-Indicator at said receiver(see fig. 3, sheet 2); encrypting a second message at said second level of encryption(see col. 3, lines 59-67, col. 4, lines 1-5); transmitting said second message at said second level of encryption; receiving said second message at said receiver; and decrypting said second message at said receiver(see col. 4, lines 7-20, 49-67).

34. As per claim 32, it is rejected under the same basis as claim 31.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are (703) ~~305-0040~~ 872-9306 for regular communications and (~~703) 308-6306~~ 703 872-9306 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

***

December 11, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100